aDvens

Security for the greater good

Cyber Threat Intelligence report Microsoft February 2024 Patch Tuesday

2024-02-15 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

aDvens

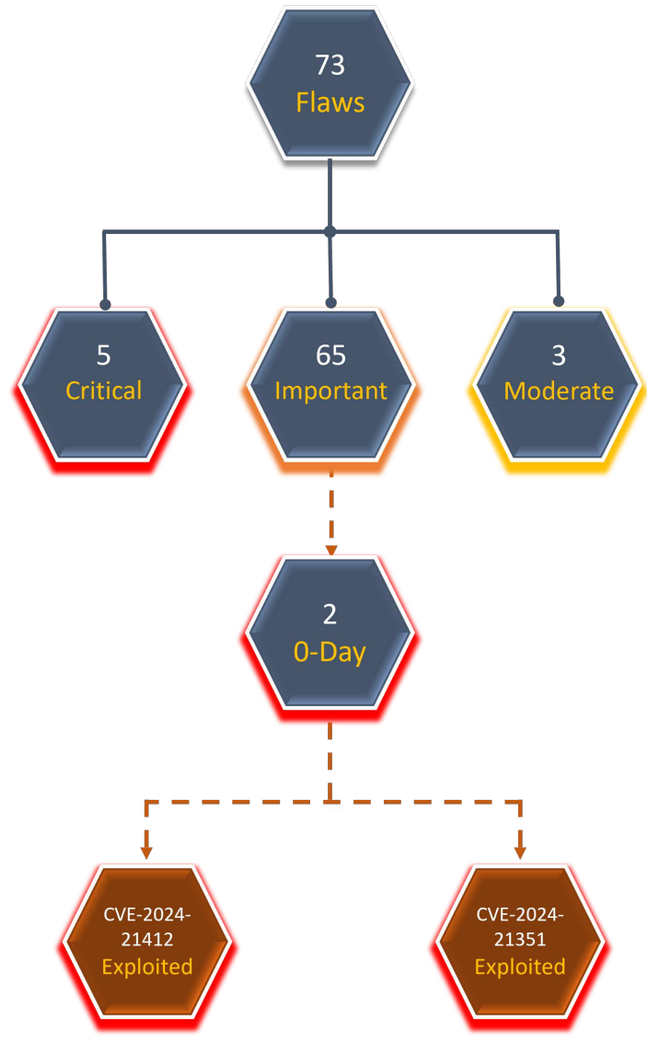
Table of content

1. Executive summary

February 2024's ***Patch Tuesday*** fixes a total of **73 vulnerabilities** including **2 exploited zero-days** : CVE-2024-21412 and CVE-2024-21351.

aDvens' CERT recommends testing proposed workaround measures in a test environment before deploying them in production. This step is crucial to prevent any unintended side effects.

Update from 15 February 2024: CVE-2024-21410 (Microsoft Exchange) has been updated following Microsoft's acknowledgement that this vulnerability is now being exploited and a proof of concept has been published for CVE-2024-21413 (Microsoft Office/Outlook). The summary table has been rectified as well.



This report highlights the following vulnerabilities that have been classified as critical :

PRODUCT	CVE	SCORE	EPSS	ZERO-DAY	EXPLOITED	CWE	POC
Internet Shortcut	CVE-2024-21412	8.1	1%	Yes	Yes	254	No
SmartScreen	CVE-2024-21351	7.6	1%	Yes	Yes	254	No
Exchange	CVE-2024-21410	9.8	0.1%	No	Yes	668	No
Office	CVE-2024-21413	9.8	0.1%	No	No	20	Yes
Azure AKS	CVE-2024-21403	9.0	0.1%	No	No	264	No

2. Internet Shortcut Files Security - CVE-2024-21412

This vulnerability is due to a link control flaw in Windows. By persuading a victim to open a specially crafted file containing *Internet Shortcut* links, an attacker can exploit this flaw to bypass security controls in order to execute arbitrary code.

User interaction is required.

This flaw has been exploited since December 2023. Researchers from *Trend Micro* have observed at least two campaigns using this vulnerability. One of these campaigns, linked to the Water Hydra (DarkCasino) group, targets the financial sector (traders). The second seems to be linked to Darkgate operators. Attackers are thought to have used phishing emails containing a link to a malicious *jpeg* image or pdf to exploit this vulnerability. When the user clicks on the image, the warning pop-up concerning potential risks is no longer displayed, and malicious files are executed until the *Remote Access Trojan* DarkMe is deployed.

2.1. Type of vulnerability

CWE-254: Security Features

2.2. Risks

- Security bypass
- Remote code execution

2.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	Required	Impact on availability	None

2.4. Impacted Products

- Windows Server 2019
- Windows Server 2022
- Windows 10
- Windows 11

2.5. Recommendations

Microsoft's February 2024 Patch Tuesday brings the necessary fixes:

KB5034768

- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for ARM64-based Systems

5034769

- Windows Server 2022, 23H2 Edition (Server Core installation)

KB5034765

- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems
- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems

KB5034770

- Windows Server 2022
- Windows Server 2022 (Server Core installation)

KB5034766

- Windows 11 version 21H2 for x64-based Systems
- Windows 11 version 21H2 for ARM64-based Systems

KB5034763

- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for ARM64-based Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 21H2 for 32-bit Systems

Additional information is available on the editor's website.

2.6. Proof of concept

To date, no proof of concept is available in open source.

2.7. Detection rules

TrendMicro have provided the following rules to help detect exploitation of the vulnerability.

```
(productCode:sds OR productCode:pds OR productCode:xes OR productCode:sao) AND eventId:1 AND eventSubId:2
AND objectCmd:"rundll32.exe" AND objectCmd:/fxbulls/ AND ( objectCmd:.url OR objectCmd:.cmd)
```

```
(productCode:sds OR productCode:pds OR productCode:xes OR productCode:sao) AND eventId:1 AND eventSubId:2
AND objectCmd:"rundll32.exe" AND objectCmd:/underwall/ AND ( objectCmd:.url OR objectCmd:.cmd)
```

```
eventId:"100101" AND (request:"*84.32.189.74*" OR request:"87iavv.com")
```

```
eventId:3 AND (src:"84.32.189.74*" OR dst:"84.32.189.74*")
```

```
productCode:(pdi OR xns OR pds OR sds OR stp OR ptp OR xcs) AND (eventId:(100115 OR 100119) OR
eventName:INTRUSION_DETECTION) AND (src:"84.32.189.74*" OR dst:"84.32.189.74*")
```

3. Windows SmartScreen - CVE-2024-21351

This vulnerability, identified as CVE-2023-36025, affects the Windows *SmartScreen* filter. This filter is used to inspect files taken from the Internet with a "*Mark-of-the-Web*" label.

By convincing a victim to open a specially crafted file, an attacker can exploit this flaw to bypass the *SmartScreen* inspection and execute arbitrary code on the system.

User interaction is required.

This vulnerability is actively exploited.

3.1. Type of vulnerability

- **CWE-254**: Security Features

3.2. Risks

- Security bypass
- Remote code execution

3.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	Low
Privileges Required	None	Impact on integrity	High
User Interaction	Required	Impact on availability	Low

3.4. Impacted Products

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

3.5. Recommendations

Microsoft's February 2024 Patch Tuesday brings the necessary fixes:

KB5034767

- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems

- Windows Server 2016

KB5034774

- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems

KB5034763

- Windows 10 Version 21H2 for 32-bit Systems
- Windows 10 Version 21H2 for x64-based Systems
- Windows 10 Version 21H2 for ARM64-based Systems
- Windows 10 Version 22H2 for 32-bit Systems
- Windows 10 Version 22H2 for x64-based Systems
- Windows 10 Version 22H2 for ARM64-based Systems

KB5034765

- Windows 11 Version 22H2 for x64-based Systems
- Windows 11 Version 22H2 for ARM64-based Systems
- Windows 11 Version 23H2 for x64-based Systems
- Windows 11 Version 23H2 for ARM64-based Systems

KB5034766

- Windows 11 version 21H2 for ARM64-based Systems
- Windows 11 version 21H2 for x64-based Systems

KB5034768

- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows Server 2019

KB5034770

- Windows Server 2022

Additional information is available in Microsoft's advisory.

3.6. Proof of concept

To date, no proof of concept is available in open source.

4. Microsoft Exchange - CVE-2024-21410

It allows an unauthenticated attacker to impersonate a user by sending *Net-NTLMv2* hashes to a vulnerable Exchange server.

Update from 15 February 2024: This vulnerability is actively exploited.

4.1. Type of vulnerability

- CWE-668: Exposure of Resource to Wrong Sphere

4.2. Risk

- Authentication bypass

4.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

4.4. Impacted Products

- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

4.5. Recommendations

Apply the following patchs :

- Microsoft Exchange Server 2016 Cumulative Update 23 and activate the *Extended Protection* fonctionality via Microsoft's script ExchangeExtendedProtectionManagement.ps1
- Microsoft Exchange Server 2019 Cumulative Update 13 and activate the *Extended Protection* fonctionality via Microsoft's script ExchangeExtendedProtectionManagement.ps1
- Microsoft Exchange Server 2019 Cumulative Update 14 : KB5035606

Microsoft also provide an article to help Exchange administrators with these updates and the Extended Protection feature, as well as a script HealthChecker.ps1 to check that the patch has been correctly applied.

Additional information is available in Microsoft's advisory.

4.6. Proof of concept

To date, no proof of concept is available in open source.

5. Microsoft Office - CVE-2024-21413

It allows an unauthenticated attacker to create a malicious link bypassing the *Protected View* protocol. This can lead to a leak of local NTLM hashes and the execution of arbitrary code.

This flaw can be exploited by viewing a specially crafted message in Outlook's preview pane.

5.1. Type of vulnerability

CWE-20: Improper input validation

5.2. Risk

- Remote code execution

5.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

5.4. Impacted Products

- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)
- Microsoft Office LTSC 2021 for 32-bit editions
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft Office 2019 for 64-bit editions
- Microsoft Office 2019 for 32-bit editions

5.5. Recommendations

Microsoft's February 2024 Patch Tuesday brings the necessary fixes.

It is necessary to apply all updates to patch the vulnerability in Microsoft Office 2016.

KB5002537, KB5002467, KB5002522, KB5002519 **and** KB5002469

- Microsoft Office 2016 (64-bit edition)
- Microsoft Office 2016 (32-bit edition)

Correctif Microsoft Office

- Microsoft Office LTSC 2021 for 32-bit editions
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft Office 2019 for 64-bit editions
- Microsoft Office 2019 for 32-bit editions
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft 365 Apps for Enterprise for 32-bit Systems

Additional information is available on the editor's website.

5.6. Proof of concept

Update from 15 February 2024: A proof of concept is available in open source.

6. Azure Kubernetes - CVE-2024-21403

Discovered by security researcher *Yuval Avrahami*, this vulnerability affects the *Confidential Container* feature of Microsoft Azure Kubernetes Service (AKS).

Confidential Container is an AKS feature, available as a *preview*, which encrypts container data at a Hardware level.

This flaw allows an unauthenticated attacker on the *AKS* cluster, by moving *Confidential Containers*, to compromise the confidentiality, integrity and availability of data.

The attacker must first control a machine in the cluster.

6.1. Type of vulnerability

- CWE-264: Permissions, Privileges, and Access Controls

6.2. Risk

- Security bypass

6.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Changed
Attack complexity	High	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

6.4. Impacted Products

- Azure Kubernetes Service Confidential Containers

6.5. Recommendations

Apply the 6 February 2024 Azure updates and install **az confcom** versions 0.3.3 or later:

- If **az confcom** is not installed, download the new version by running the command **az extension add -n confcom**.
- If **az confcom** is already installed, update it by running the command **az extension add -n confcom**.

6.6. Proof of concept

To date, no proof of concept is available in open source.

7. Indicators of compromise (CVE-2024-21412)

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/xampp/	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/webdav/	
TLP:CLEAR	URL	hxxps://fxbulls[.]ru	
TLP:CLEAR	URL	hxxps://fxbulls[.]ru/wp-content/uploads	
TLP:CLEAR	URL	hxxps://fxbulls[.]ru/wp-content/uploads/2023/12/photo_2023-12-29[.]jpg[.]htm	
TLP:CLEAR	URL	hxxps://fxbulls[.]ru/wp-content/uploads/2023/12/photo_2023-12-29[.]jpg[.]html	
TLP:CLEAR	URL	hxxps://84[.]32[.]189[.]74@0[.]0[.]0[.]80/fxbulls/net/2[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/photo_2023-12-29[.]jpg[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/Thumbs[.]db	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/2[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip/a2[.]cmd	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/b3[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/7z[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/7z[.]exe	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/photo_2023-12-29s[.]jpg	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/pictures/My2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/photo_2023-12-29[.]jpg[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/Thumbs[.]db	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/2[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/a2[.]zip	

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/a2[.]zip/a2[.]cmd	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/b3[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/7z[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/7z[.]exe	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/photo_2023-12-29s[.]jpg	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/images/My2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/photo_2023-12-29[.]jpg[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/Thumbs[.]db	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/2[.]url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/a2[.]zip/a2[.]cmd	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/a2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/b3[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/7z[.]dll	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/7z[.]exe	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/photo_2023-12-29s[.]jpg	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/fxbulls/net/My2[.]zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/docs	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/docs/7z.zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/docs/passport.jpg.url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/docs/warop.url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/expand	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/expand/7z.zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/expand/photo_2023-12-26.jpg.url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/expand/warop.url	

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/society	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/society/7z.zip	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/society/photo_2023-12-26.jpg.url	
TLP:CLEAR	URL	hxxp://84[.]32[.]189[.]74/underwall/society/warop.url	
TLP:CLEAR	Domain	fxbulls[.]ru	
TLP:CLEAR	Domain	87iavv[.]com	
TLP:CLEAR	Domain	unfawjelesst322[.]com	
TLP:CLEAR	Domain	p2oaviwt39ui[.]com	
TLP:CLEAR	IP	84[.]32[.]189[.]74	
TLP:CLEAR	IP	179[.]43[.]172[.]127	
TLP:CLEAR	IP	179[.]43[.]172[.]191	
TLP:CLEAR	IP	64[.]31[.]63[.]70	
TLP:CLEAR	IP	64[.]31[.]63[.]194	
TLP:CLEAR	SHA-256	1458a762332676f7807ab45f8f236c22a1a7bb0c21fcd8c779f972f2446a11d0	Trojan.HTML.CVE202421412.A
TLP:CLEAR	SHA-256	758c6364ab560fbeff2bfa8712a2e09132d85d0bf6918e6acc79fe12f5b71ec3	Trojan.HTML.CVE202421412.A
TLP:CLEAR	SHA-256	77d685e29c3dbe75fa8a82c69c68c731a09904020a76145ca27aeaf0058455cd	Trojan.HTML.CVE202421412.A
TLP:CLEAR	SHA-256	b36dc329a5dc766c2645d5f5b6cdaa9542ec3b0aa1bc13dc1f899ce6d95d59fb	Trojan.HTML.CVE202421412.A
TLP:CLEAR	SHA-256	d895fff3c909ea2eb6624fc5f154c924fe0af51c6c899fd9093dc3cd27a5dad2	Trojan.HTML.CVE202421412.A
TLP:CLEAR	SHA-256	008e57d62caa8cfa991f5519eabe3f15d79799b81ba8cc6b67cde6da0dbffdab	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	087878208755420d5d7ae2eb6a84482768cb8972732911ac16096cd0c95fa0f7	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	1115e4bed3949493d8ab184e5c42f047355f13b9bf91c1621acb7971a148bea2	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	18b1dc2e00245cb017ebdedfe63881929d7542eeffa8f42ee0ad20cc2ebf181a	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	1956bcd3df47e76b2e9f396514f072311563d092ae02509f817c488567749998	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	1fbc621a71578cb22d4e3a0feec68735321358a3aeb18adbe4a20630c7f788b8	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	39fb9fb06910f1133f3b23c523a5139f61d243380802b0670a664473d00e1fa9	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	3e420ce1dc1a8503f48815b880381dd23206e08be2474d151f1353df7df2d796	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	4201ab8c0c4cf0f01f5a25d8e4e7221634776b5bad8c3faad5ad819ec58619ad	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	58b0f5da4a53e956b35e77f55ced641291a596e16067b1dab6ac54d9cb6a52a5	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	5b16ac1edb747053ee5a085ab826c61218c5b471eaa04f2471dc2e80b5621023	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	5c85a0fe230d351b35da364c797cc95557f5dcceec034eb648e1805237c7203b	Trojan.Win32.CVE202421412.A

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	SHA-256	5f4ef55201080ef3a62b0fbdc4c27e0ccdf4041f41c04471f35b127ff6515405	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	61de01bc154b1118caacfed3839c996a795d6c21c2efbf1da6b926414f5d182d	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	65cc5594b307c2ac4e3c251aeae68dedf7d1f24ba3b0d7ab5ad3623e8a9fc865	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	6793e0fbc2def9173bf8e2a6c1aa357ba7fc3e32dc1cf81107677166f175c890	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	6bec457f83d0d98f6f6ea1243c2327e012db38fb61680f6bd68dbab0dc07170a	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	7058ae0f02e116b38536ee1ec20f47645aecf761361b5a5e85de2961f3cc88c6	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	70b4c2d696a24a5ae2f5e5095dc44e68b4605e4690c8a49930194ee87eb80252	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	73922ab0d048b45a01f13ba967f1423bc6cd6cc711f8e7d00a4cf2b1d3646f4e	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	761fa42bc4cc5332a640c7389240324242981176ca1626e4267cc8a00cf9545f	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	88bb1df99e02021801b08beeff87ec3ceb9e16c42f62904c5ac04c1a26213a48	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	941cf63028bf8314bc7114a088f4d1f1dd995bec4a4b7c51fda34fbb3528667f	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	a45e0ea5a17ba6f3a2ce7258f6cc81c6f93f37873b49218a25ec638987da6f96	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	a5096c4624a523a660242e3451c2f4d644431a35098e36b724fab9f7d88d145d	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	a9633da58719f07159702101474b6ba78f2ffee28b3f7ebda3feb36db4e2d0e9	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	b0ab19986ab1297870854980f1287f1a4b8d003c540773a6c04fb3565e5701ee	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	b350a787c19a756c0824e14eec7e9d746450d1aafb28a5d15209ec9f34c58129	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	b738e92afc95cba819aa7aebfad459de38743c478e9e8b8f29f9919697b495b0	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	b8b6b6d98b7ea689f0c33d55a06afcf20482b25c51929ca9a1b302374290b337	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	babbd9c94dedb94be8baac2ddc5b4714c44a8d0c60d49c0dc91708784bc0d57f	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	bbdf52481bd1a15710d75b89240c7a360450e2f4f00ba2cb140affba79ebec94	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	c86ba0da732e1fa1f06549d3ebc5ae6ae091199e95930681ac2a9152a8834184	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	d6000a19198b8b9719fc17f7c06366e542802a8e7e232ba731b72c31226cc890	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	d81e7d95004441ea4f5344215232db57f48579bf335c7ba4ed7f6ec6f9136ed0	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	db1bc70c0d0c7121f1d4422a6fcd0e0668d9da786affb52dd77852641e425710	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	ddda5737b2c3207d72d728bf40709a7296c31e7c50951dcad441f4707581ccb1	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	e1b903eba88b920909876442306e1160eed9b69c69a05ea370cba2121e305ba1	Trojan.Win32.CVE202421412.A

TLP	TYPE	VALUE	COMMENT
TLP:CLEAR	SHA-256	e49a7d9083b2e448274d117405c39b0c1b2c0c20ab5195bdf94aaeda7cc113d7	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	f44964c8fdf6dbdb21c141df61b45467bba5a4482f7ab19fd6f1841fdb791f2a	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	f6b01df60d526f1de530230724d41b482adfff81084a1872bb97c316b76e45e3	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	f701f500d348b63f3250239cd8305a8b38230e67d74456f3333c6efeeef85bbb	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	fb67be10a5a8b26ca86f8f79935ddd4a5b40379bb6d0af21d23f56af14bb2a90	Trojan.Win32.CVE202421412.A
TLP:CLEAR	SHA-256	4307a067db6b6abd852441e6d70de29c3bd0e4d6a68f0449b403401518b7e037	Trojan.Win32.CVE202421412.B
TLP:CLEAR	SHA-256	69fc5bed55acf559035f2c5550bf8807236b580f8e2db88966b3fc80c83914d3	Trojan.Win32.CVE202421412.B
TLP:CLEAR	SHA-256	4c43b4575063d50ca5668e45a434aaf288970c89e8a4414812560ee787307f58	Trojan.Win32.CVE202421412.B
TLP:CLEAR	SHA-256	135cfefe353ca57d24cfb7326f6cf99085f8af7d1785f5967b417985e8a1153c	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	252351cb1fb743379b4072903a5f6c5d29774bf1957defd9a7e19890b3f84146	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	594e7f7f09a943efc7670edb0926516cfb3c6a0c0036ac1b2370ce3791bf2978	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	6e825a6eb4725b82bd534ab62d3f6f37082b7dbc89062541ee1307ecd5a5dd49	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	71d0a889b106350be47f742495578d7f5dbde4fb36e2e464c3d64c839b1d02bc	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	b69d36e90686626a16b79fa7b0a60d5ebfd17de8ada813105b3a351d40422feb	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	bf9c3218f5929dfeccbbdc0ef421282921d6cbc06f270209b9868fc73a080b8c	Trojan.Win32.DARKME.A
TLP:CLEAR	SHA-256	dc1b15e48b68e9670bf3038e095f4afb4b0d8a68b84ae6c05184af7f3f5ecf54	Trojan.Win32.DARKME.A

8. Sources

- https://www.zerodayinitiative.com/blog/2024/2/13/the-february-2024-security-update-review
- https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2024-patch-tuesday-fixes-2-zero-days-73-flaws/

Microsoft Internet Shortcut Files Security - CVE-2024-21412

- https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html
- https://www.zerodayinitiative.com/blog/2024/2/13/the-february-2024-security-update-review
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412
- https://www.cve.org/CVERecord?id=CVE-2024-21412
- https://thecyberexpress.com/cisa-flags-2-critical-windows-vulnerabilities/

Windows SmartScreen - CVE-2024-21351

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21351
- https://www.cve.org/CVERecord?id=CVE-2024-21351

Microsoft Exchange - CVE-2024-21410

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410
- https://www.cve.org/CVERecord?id=CVE-2024-21410
- https://thehackernews.com/2024/02/critical-exchange-server-flaw-cve-2024.html

Microsoft Outlook - CVE-2024-21413

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413
- https://www.cve.org/CVERecord?id=CVE-2024-21413

Azure Kubernetes - CVE-2024-21403

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21403
- https://www.cve.org/CVERecord?id=CVE-2024-21403